PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH FORESCOUT COUNTERACT®

Attivo Networks has partnered with ForeScout Technologies, Inc. to provide advanced real-time in-network threat detection and improve automated incident response to block and quarantine infected endpoints. With the joint solution, customers can review alerts and have the choice to make manual updates or alternatively to create policies to automatically block endpoints based on suspicious activity. Customers can reduce time and resources required to detect threats, analyze attacks, and to remediate infected endpoints, ultimately reducing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Expedited Incident Response
- End-point Deception Credentials Distribution

THE CHALLENGE

Cyberattackers have repeatedly proven that they can and will get inside the networks of even the most security-savvy organizations. Whether the attacker finds their way in through the use of stolen credentials, zero-day exploitation, a ransomware attack or simply start as an insider, they will establish a foothold and will move laterally throughout the network until they can complete their mission.

Once attackers bypass the existing security prevention mechanisms they can easily move around the network undetected by existing security solutions. To quickly detect and shut down these attacks, a new approach to security is needed. This approach focuses on the threats that are inside the networks and does not use typical measures such as looking for known signatures or attack pattern matching. This new method to detect attacks uses deception to deceive attackers into revealing themselves and once engaged, can capture valuable attack forensics that can be used to promptly block the attacker from continuing or completing their mission.

THE ATTIVO THREATDEFEND PLATFORM AND FORESCOUT COUNTERACT JOINT SOLUTION

The integration of the Attivo ThreatDefend Deception Platform with ForeScout CounterACT is very simple to set up. In minutes, organizations can have an integrated adaptive security platform that provides effective prevention, real-time detection of cyberattackers, and automatic blocking and quarantine of infected systems to effectively stop data exfiltration and contain the attack. The integrated solution provides a real-time, non-disruptive way of detecting and blocking BOTs and APTs inside the network, closing the opportunity for an attacker to exfiltrate valuable company assets and information. Automating remediation is

becoming critically important as malware lateral movement speeds increase. The combination of the Attivo BOTSink® Engagement Server and ForeScout CounterACT provides real-time remediation capabilities that outperform systems that depend upon manual intervention.

ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the solution provides network, endpoint, and data deceptions and is highly effective in detecting threats from all vectors such as reconnaissance, stolen credentials, Man-in-the-Middle, Active Directory, ransomware, and insider threats. The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink engagement servers, decoys, lures, and breadcrumbs, the ThreatStrike™ endpoint deception suite, ThreatPath™ for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM) which together create a comprehensive early detection and active defense against cyber threats.

SUMMARY

The Attivo ThreatDefend Platform plays a critical role in empowering an active defense with in-network threat detection and integrations to dramatically accelerate incident response.

By identifying the source of breach attempts, the Attivo ThreatDefend Platform can be configured to send compromised endpoint alerts directly to ForeScout CounterACT. Policies configured in CounterACT can then automatically quarantine the endpoint by reventing network access. The time saved in blocking malicious traffic on the network is critical to preventing lateral movement and data exfiltration. A strategy that depends upon manual intervention may work for lowseverity alerts. High-severity attacks may not afford security teams the benefit of time to react to these alerts. Automation of blocking and quarantining give the advantage back to the security team and will help contain the attack before mass damage or exfiltration can be done. The need for this integration is urgent. In a single year, over one billion sensitive records have been stolen with detrimental impact to individuals and enterprises. The resulting damage to the companies' reputations and balance sheets has reached into the billions of dollars. By implementing solutions that detect in-network threats early and having the ability to automatically block and quarantine those threats, organizations can mitigate the risk of large-scale breaches.

ABOUT ATTIVO NETWORKS

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

ABOUT FORESCOUT TECHNOLOGIES

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional endpoints, IoT devices and operational technologies the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments.

www.forescout.com